WHAT IS CLAIMED IS:

1. A semiconductor integrated circuit device comprising:

a first memory for inputting and outputting data between a bus and itself;

a second memory for inputting and outputting data between the bus and itself;

a secret key holder for holding a secret key;

a bus port for controlling access from outside to the bus;

a CPU for storing an encrypted program and a decryption program in the first memory via the bus port, decrypting the encrypted program by using the decryption program and the secret key, and executing the decrypted program; and

a controller for causing, when the encrypted program and the decryption program are stored in the first memory, the bus port to disable access from the outside, enabling access to the first and second memories, and thereby transferring the encrypted program and the decryption program from the first memory to the second memory,

disabling access to the first memory when the transfer is completed, and

disabling access to the second memory when the decryption and the execution of the decrypted program are completed.

2. The semiconductor integrated circuit device of claim 1, further comprising:

a secret key access port for controlling access from the CPU to the secret key holder, wherein

the secret key access port enables access to the secret key holder when the transfer is completed and disables access to the secrete key holder when the execution of the decrypted program is completed.

3. The semiconductor integrated circuit device of claim 1, wherein the CPU includes a register and erases data stored in the register if the execution of the decrypted program is completed.

4. The semiconductor integrated circuit device of claim 1, wherein the controller controls access to the first and second memories by controlling chip select signals to the first and second memories.

5. The semiconductor integrated circuit device of claim 1, wherein

the controller includes a flag storing portion for storing first and second flags, enables access to the first and second memories when the first flag is set, disables access to the first memory when the first flag is reset and the second flag is set, and disables access to the second memory when each of the first and second flags is reset,

the bus port disables access from the outside when at least one of the first and second flags is set, and

the CPU sets the first and second flags when the encrypted program and the decryption program are inputted to the first memory, resets the first flag when the transfer is completed, and resets the second flag when the execution of the decrypted program is completed.

6. A semiconductor integrated circuit device comprising:

a first memory for inputting and outputting data between a bus and itself;

a second memory for inputting and outputting data between the bus and itself;

a first memory port connected between the bus and the first memory to control access from the bus to the first memory;

a second memory port connected between the bus and the second memory to control access from the bus to the second memory;

a secret key holder for holding a secret key;

a bus port for controlling access from outside to the bus;

a CPU having a register, the CPU writing an encrypted program and a decryption program in the first memory via the bus port, decrypting the encrypted program by using

the decryption program and the secret key, writing the decrypted program in the second memory, and executing the decrypted program; and

a controller for causing, when the writing to the first memory is completed, the bus port to disable access from the outside to the bus, causing the first memory port to disable the writing to the first memory, and causing the second memory port to enable access to the second memory and

causing, when the execution of the decrypted program is completed, the CPU to erase data stored in the register and disable access to the secrete key holder, while causing the second memory port to disable access to the second memory.

7. A semiconductor integrated circuit device comprising:

a first memory for inputting and outputting data between a bus and itself;

a second memory for inputting and outputting data between the bus and itself;

a memory port connected between the bus and the first memory to control access from the bus to the first memory;

a secret key holder for holding a secret key;

a bus port for controlling access from outside to the bus;

a CPU having a register, the CPU writing an encrypted program and a decryption program in the first memory via the bus port, decrypting the encrypted program by using the decryption program and the secret key, writing the decrypted program in the second memory, and executing the decrypted program; and

a controller including a memory initializer for erasing data in the second memory, the controller causing, when the wiring to the first memory is completed, the bus port to disable access from the outside to the bus and causing the memory port to disable the writing to the first memory and

causing, when the execution of the decrypted program is completed, the CPU to

erase data stored in the register and disable access to the secret key holder and causing the memory initializer to erase the data in the second memory.

8. A semiconductor integrated circuit device comprising:

a first memory for inputting and outputting data between a bus and itself;

a second memory for inputting and outputting data between the bus and itself;

a secret key holder for holding a secret key;

a decryption key holder for holding a decryption key;

a bus port for controlling access from outside to the bus;

a CPU including a register, the CPU performing first storage for storing the encrypted decryption key and a decryption key decryption program in the first memory via the bus port, performing first decryption for decrypting the encrypted decryption key by using the decryption key decryption program and the secret key, writing the decrypted decryption key in the decryption key holder, performing second storage for storing an encrypted program and a decryption program in the first memory, performing decryption for decrypting the encrypted program by using the decryption program and the decrypted decryption key, and executing the decrypted program; and

a controller for causing, when the first storage to the first memory is completed, the bus port to disable access from the outside to the bus and enabling access to the first and second memories such that the encrypted decryption key and the decryption key decryption program are transferred from the first memory to the second memory,

enabling, when the transfer is completed, access to the secret key holder and disabling access to the first memory;

causing, when the first decryption is completed, the CPU to erase data stored in register and disable access to the secret key holder, while disabling access to the second memory, enabling access to the first memory, and causing the bus port to enable access

from the outside to the bus,

causing, when the second storage to the first memory is completed, the bus port to disable access from the outside to the bus and enabling access to the second memory such that the encrypted program and the decryption program are transferred from the first memory to the second memory,

enabling, when the transfer is completed, access to the decryption key holder and disabling access to the first memory, and

causing, when the second decryption and the execution of the decrypted program are completed, the CPU to erase data stored in the register and disable access to the secret key holder and disabling access to the second memory.

9. A program delivery method for delivering a program between a first device and a second device, the method comprising the steps of:

transferring a public key from the second device to the first device;

transferring a decryption program to the second device from the outside thereof;

encrypting the program by using the public key in the first device and transferring the encrypted program to the second device; and

decrypting the encrypted program by using a secret key corresponding to the public key and the decryption program in the second device.

10. A program delivery method for delivering a program between a first device and a second device, the method comprising the steps of:

transferring a public key from the second device to the first device;

encrypting a decryption key by using the public key in the first device and transferring the encrypted decryption key to the second device;

decrypting the encrypted decryption key by using a secret key corresponding to the public key in the second device;

encrypting the program by using an encryption key corresponding to the decryption key in the first device and transferring the encrypted program to the second device; and

decrypting the encrypted program by using the decrypted decryption key in the second device.

11. A program delivery system for delivering a program, the system comprising:

a first device and a second device,

the first device encrypting the program by using a public key and transferring the encrypted program to the second device and

the second device decrypting the program encrypted by the first device by using a secret key corresponding to the public key and a decryption program transferred from the outside of the second device.

12. A program delivery system for delivering a program, the system comprising:

a first device and a second device,

the first device encrypting a decryption key by using a public key, transferring the encrypted decryption key to the second device, encrypting the program by using an encryption key corresponding to the decryption key, and transferring the encrypted program to the second device,

the second device decrypting the decryption key encrypted by the first device by using a secret key corresponding to the public key and decrypting the program encrypted by the first device by using the decrypted decryption key.